МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ
УКРАЇНСЬКИЙ ІНСТИТУТ ПРОМИСЛОВОЇ ВЛАСНОСТІ
(УКРПАТЕНТ)

Україна, 04119, м. Київ-119, вул. Сім'ї Хохлових, 15, тел./факс 458-06-11,
Україна, МСП 04655, м. Київ-53, Львівська площа, 8, тел. 212-50-82, факс 212-34-49

№ 862/01 від "01" 07 2002 р.

Міністерство освіти і науки України цим засвідчує, що

додані матеріали є точним відтворенням первісного опису,

формули і креслень заявки № **2002032465** на видачу патенту на

винахід, поданої **28.03.2002**

Назва винаходу: СПОСІБ ЗАХИСТУ ПАМ'ЯТІ КОМП'ЮТЕРІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ І ПРИСТРІЙ ДЛЯ ЙОГО ЗДІЙСНЕННЯ

Заявник: Шевченко О.Ю.

Дійсний автор: Шевченко О.Ю.

УКРАЇНА

За дорученням Державного департаменту інтелектуальної власності

А.Красовська

МПК[7] G 06 F 12/14

СПОСІБ ЗАХИСТУ ПАМ'ЯТІ КОМП'ЮТЕРІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ І ПРИСТРІЙ ДЛЯ ЙОГО ЗДІЙСНЕННЯ

Галузь техніки

Винахід відноситься до методів захисту пам'яті комп'ютерів від несанкціонованого доступу сторонніх користувачів через довільні канали зв'язку і до структури пристроїв для реалізації таких методів.

Слід мати на увазі, що *стосовно до винаходу* тут і далі позначені:

терміном «*комп'ютер*» - переважно персональний комп'ютер (далі ПК), що самостійно або в локальній мережі працює в режимі вільного обміну даними з іншими комп'ютерами через довільний канал зв'язку і, особливо, через *Internet*;

терміном «*пам'ять комп'ютера*»:

- такі апаратні засоби, як вбудовані в комп'ютер довгочасні (далі ДЗП) і оперативні (далі ОЗП) запам'ятовуючі пристрої, і

- такі набори даних, як бази даних (далі БД) і/або бази знань (далі БЗ) і/або інстальоване програмне забезпечення (далі ПО), включаючи системи керування базами даних і/або знань, що зберігаються на зазначених апаратних засобах;

терміном «*постійний запам'ятовуючий пристрій (далі ПЗП)*» - щонайменше один такий зв'язаний з зовнішнім контролером пристрій для зберігання програмного забезпечення, яке призначене для обробки (особливо, для сортування і тестування) будь-яких вхідних повідомлень незалежно від ЦП, ДЗП й ОЗП комп'ютера, що захищається;

терміном «*захист*» - виключення несанкціонованого доступу через довільні відкриті канали зв'язку до пам'яті будь-якого комп'ютера і, відповідно, виключення крадіжок і/або псування і/або зміни ПО і/або БД і/або БЗ;

терміном «*сторонній користувач*» - будь-який хакер, але переважно кракер, який сам або за замовленням прагне активно вплинути на роботу чужого комп'ютера.

Рівень техніки

Загальновідомо, що в пам'яті сучасних комп'ютерів зберігаються гігантські кількості такої інформації, ушкодження, утрата, або розголошення якої можуть спричинити серйозні економічні і/або політичні втрати. Тому псування ПО і, особливо, БД або БЗ комп'ютерними вірусами і крадіжок або змін даних давно стали серйозною загрозою навіть власникам домашніх

ПК і, тим більше, корпораціям, окремим державним органам і державам у цілому.

Дійсно, власники комп'ютерів нерідко страждають від вірусів, які вони звичайно випадково одержують або з *Internet*, або разом з листами по електронній пошті, або при обміні даними з іншими користувачами з застосуванням дискет і інших засобів автономного зберігання і передачі даних. І хоча розробка і розсилання нових вірусів звичайно представляють собою нецілеспрямоване хуліганство, воно тим більше небезпечно, чим гірше підготовлені до вірусних атак окремі користувачі.

Ще більш небезпечний навмисний цілеспрямований злом БД корпорацій, банків і державних установ кракерами. Вони нерідко працюють по замовленнях конкурентів або терористів, використовуючи усе більш витончені програмні засоби злому типу «хробаків» і/або «троянських конів». У сучасному світі особливо небезпечний злом воєнних систем інформаційного забезпечення і керування військами, що може відкрити несподівані можливості для вчинення терористичних актів.

З сказаного ясно, що засоби протидії зазначеним загрозам повинні бути якомога ефективніші незалежно від джерела і характеру загрози, загальнодоступні користувачам комп'ютерів за ціною, надійні, прості і зручні в застосуванні.

На жаль, на сьогодні лише деякі з цих вимог можуть бути ефективно виконані.

Наприклад, загальновідомі такі засоби зниження імовірності несанкціонованого доступу до пам'яті комп'ютерів, як буквені, цифрові і буквено-цифрові паролі. Вони дешеві, прості і зручні в застосуванні.

Однак у міру розвитку хакерства з'ясувалося, що такі «словесні» паролі є помітною перешкодою лише для починаючих користувачів. Дійсно, нині навіть істотно дорожчі в застосуванні іконічні паролі типу відбитків пальців або райдужної оболонки ока законного користувача комп'ютера не рятують від злому. Мало того, ніякі паролі не рятують ПО, БД і БЗ від зараження вірусами і псування.

Зрозуміло, що створення і поширення антивірусів, а останнім часом - і антивірусних програмних комплексів з евристичними компонентами зменшує втрати від псування ПО, БД і БЗ. Однак цей шлях ефективний лише при атаках тими вірусами, що були ідентифіковані і проти яких вже створені антивіруси.

Інший загальновідомий метод зниження імовірності несанкціонованого доступу до пам'яті комп'ютерів заснований на застосуванні криптографії (див. розділ «Конспирация - вымысел

и реальность» у книзі Д. Вакка «Секреты безопасности в *Internet*.- Киев: ДИАЛЕКТИКА, 1997» / Internet Security SECRETS by John R. Vacca, IDG Books Worldwide, Inc.).

На жаль, цей метод придатний для безпечного обміну даними лише між добре відомими друг другу користувачами, коло яких дуже вузьке, і при використанні кодів, які містять більш 128 біт. Це робить захист комп'ютерів набагато дорожчим і різко звужує можливості обміну інформацією через довільні канали зв'язку.

Тому фахівці усе частіше прагнуть спорудити між окремими ПК і загальнодоступними відкритими каналами зв'язку такі перепони, які образно називають «*брандмауерами*» (див., наприклад, у *Internet* за адресою <IRL: http://www.esafe.com/press/pr032997.html> статтю «New anti-vandal software provides Next Generation PC Protection»).

Кожний сучасний брандмауер є програмно-апаратним комплексом, який фільтрує вхідні повідомлення (наприклад, мережний трафік), виділяє (за заздалегідь обраними критеріями) підозрілі повідомлення й або припиняє їх доступ у зону захисту, або тимчасово ізолює їх, наприклад, у «пісочниці», для наступної перевірки поза контактом з власною БД або БЗ.

Так, із US 6,275,938 відомий спосіб перевірки підозрілих програм, що написані для прямого виконання на комп'ютерній платформі з модулями пам'яті й інтерфейсу. Цей спосіб включає:

виділення в ДЗП комп'ютера заздалегідь визначеної обмеженої зони пам'яті («пісочниці») для запису і зберігання підозрілих програм,

завантаження таких програм у зазначену пісочницю,

уведення контрольного коду в кожну підозрілу програму для блокування зовнішніх зв'язків зазначеної пісочниці,

заміну зв'язків у коді для модуля інтерфейсу зв'язками з модулем перекодування для придушення і блокування спрацьовування деяких частин модуля інтерфейсу і

контрольне виконання підозрілої програми.

Така перевірка передбачає використання власних апаратних і програмних ресурсів комп'ютера, що захищається. Тому навіть тоді, коли користувачі комп'ютерів, що захищаються, активно управляють перевіркою, професійні кракери здатні пробити брандмауер. Мало того, носіями хробаків і троянських конів можуть виявитися не тільки підозрілі програми, але і зовні невинні текстові і/або іконічні повідомлення, що відбираються з *Internet*.

Більш ефективні брандмауери, які:

автоматично включаються при розпізнаванні в повідомленнях, що надходять по каналах зв'язку, таких паттернів діяльності, які свідчать про спроби прориву системи безпеки (US 6,304,975), або

оснащені добре відомими фахівцям додатковими інтерфейсами введення-виведення даних з застосуванням кодів типу «свій-чужий».

Однак автоматично керовані програмні брандмауери неефективні, якщо кракери використовують засоби злому, що не були враховані в програмі захисту, а застосування зазначених кодів реально можливо тільки у відносно замкнутих мережах типу *Ethernet*, де кожний користувач перед підключенням одержують код «свій».

Тому створення брандмауерів для таких ПК або комп'ютерних систем, що змушені працювати в режимі вільного обміну даними з іншими комп'ютерами через довільні канали зв'язку і, особливо, через *Internet*, залишається актуальною проблемою.

Для цього бажано застосовувати додаткові апаратні засоби з власним програмним забезпеченням. З них, по наявним даним, до запропонованих далі засобів такого типу найбільше близькі спосіб і пристрій для захисту пам'яті комп'ютерів від несанкціонованого доступу сторонніх користувачів через *Internet* (див. US 6,061,742).

Відомий спосіб заснований на поділі даних, одержуваних із зовнішньої мережі по загальнодоступних каналах зв'язку, і команд керування обробкою даних, які надходять від комп'ютера, що захищається.

Для реалізації способу запропонований проміжний мережний адаптер, який має:

перший інтерфейс для обміну даними між зовнішньою мережею і цим адаптером,

другий інтерфейс для обміну даними між цим адаптером і власним мережним інтерфейсом комп'ютера, що захищається, і

зовнішній контролер (процесор), що зв'язаний з зазначеним мережним адаптером і призначений для поділу даних, одержуваних із зовнішньої мережі через перший інтерфейс, і команд, що надходять від комп'ютера, що захищається, через другий інтерфейс.

Таке збільшення кількості «посередників» між окремими комп'ютерами (у тому числі, включеними в локальну мережу з загальним центром керування) і зовнішньою мережею знижує імовірність несанкціонованого доступу до даних, що захищаються, через Telnet, FTP або SNMP, але не виключає злом БД і/або БЗ і/або псування ПО при використанні інших мережних протоколів. Дійсно, відомий винахід не передбачає повну ізоляцію ДЗП й ОЗП комп'ютера, що

захищається, від атак ззовні.

Суть винаходу

У основу винаходу покладена задача удосконаленням процедури обміну даними створити такий спосіб і такий пристрій захисту від несанкціонованого доступу, що могли б практично виключити вхід сторонніх користувачів у ДЗП й ОЗП комп'ютерів, що захищаються, при вільному обміні довільними даними через довільний канал зв'язку.

Ця задача вирішена тим, що в способі захисту пам'яті комп'ютерів від несанкціонованого доступу, що заснований на поділі даних, одержуваних по загальнодоступних каналах зв'язку, і команд керування обробкою даних, що надходять від комп'ютера, що захищається, з застосуванням зовнішніх апаратних засобів, *згідно з винаходом*

а) у кожному сеансі зв'язку усі вхідні повідомлення спочатку записують на щонайменше один замкнений з боку комп'ютера, що захищається, зовнішній запам'ятовуючий пристрій (далі ЗЗП);

б) потім замикають вхід у ЗЗП з боку каналу зв'язку;

в) під керуванням зовнішнього контролера з власним програмним забезпеченням незалежно від ЦП, ДЗП й ОЗП комп'ютера, що захищається, сортують непусту множину отриманих повідомлень і виділяють із неї щонайменше одну непусту підмножину файлів, яка належить до групи підмножин, що складається з:

першої підмножини файлів, імена яких мають стандартні розширення, що вказують на текстовий і/або іконічний характер цих файлів, і/або

другої підмножини файлів, імена яких мають стандартні розширення, що вказують на програмний характер цих файлів, і/або

третьої підмножини файлів, імена яких мають нестандартні розширення і які можуть бути віднесені до першої або другої з зазначених підмножин після додаткового аналізу; і

г) під керуванням зазначеного зовнішнього контролера також незалежно від ЦП, ДЗП й ОЗП комп'ютера, що захищається, обробляють повідомлення в кожній з зазначених підмножин для визначення потреби в їх одержанні і допустимості їх включення у БД і/або БЗ і/або ПО комп'ютера, що захищається.

Оскільки таку обробку всіх отриманих повідомлень проводять у зовнішній «пісочниці» на основі ЗЗП з входами-виходами, що блокуються, остільки на вході в кожний комп'ютер або локальну комп'ютерну мережу, що захищається, при малих витратах програмних і апаратних

засобів удається створити практично непробивний брандмауер. Дійсно, при будь-якій кількості послідовних атак ззовні будь-які повідомлення надходять на комп'ютер, що захищається, тільки через ЗЗП, усі записи в якому після кожного сеансу зв'язку стираються. Аналогічно, усі виходи в зовнішні канали зв'язку відбуваються через ЗЗП при заблокованому інтерфейсі комп'ютера, що захищається.

Тому робота в режимі «запит-відповідь» практично виключена.

Перша додаткова відмінність полягає в тому, що кожне отримане повідомлення, що є текстовим і/або іконічним файлом із зазначеної першої підмножини, виводять через відеоадаптер на дисплей тільки в графічному режимі у вигляді набору пікселів, оцінюють потребу в отриманому повідомленні і далі:

при позитивній оцінці - перетворюють набір пікселів в активному вікні дисплея в стандартний текстовий і/або графічний формат і це перетворене повідомлення безпосередньо з активного вікна дисплея записують у ДЗП комп'ютера, що захищається, і відповідний запис у ЗЗП стирають, а

при негативній оцінці - активне вікно дисплея закривають без зберігання даних і запис відповідного повідомлення у ЗЗП стирають.

Перетворення текстових і/або іконічних файлів у набір пікселів і повторне перетворення цього набору пікселів у придатний стандартний текстовий і/або графічний формат щонайменше дезактивує, а в більшості випадків знищує будь-які віруси і будь-яких хробаки або троянські коні і т.п. «доповнення», які хакери і кракери використовують для несанкціонованого доступу до пам'яті чужих комп'ютерів.

Друга додаткова відмінність полягає в тому, що зазначений набір пікселів, що представляє текстовий і/або іконічний файл, формують з використанням стандартних команд керування екраном. Це дозволяє різко зменшити витрати апаратних і програмних ресурсів на зазначене пряме і зворотне перетворення і навантаження на тракти передачі даних, оскільки щонайменше фон для тексту і/або зображення задається одною командою. Аналогічно, використання таких команд дозволяє більш ощадливо представляти тексти і зображення, у яких присутні стандартні елементи.

Третя додаткова відмінність полягає в тому, що використовують відеоадаптер і дисплей комп'ютера, що захищається. Це дозволяє спростити зовнішню стосовно комп'ютеру, що захищається, апаратну частину брандмауера, не знижуючи ефективності захисту від злому.

Четверта додаткова відмінність полягає в тому, що в імені кожного програмного файла з зазначеної другої підмножини стандартне розширення заміняють нестандартним розширенням, виконують пробний запуск такого файла переважно поза комп'ютером, що захищається, оцінюють потребу в отриманій програмі і далі:

при позитивній оцінці - записують прийняту програму в ДЗП комп'ютера, що захищається, і стирають запис висхідного повідомлення у ЗЗП, а

при негативній оцінці - стирають запис непотрібного висхідного повідомлення у ЗЗП.

Навіть тоді, коли сумнівна програма, що містить хробака і/або троянського коня, буде перевірена в комп'ютері, що захищається, і прийнята, зазначені засоби злому виявляться законсервованими в пам'яті комп'ютера, що захищається, тому що він може приймати чергові повідомлення ззовні тільки через ЗЗП, яке блокується, і не може автоматично відповідати на запити сторонніх користувачів.

П'ята додаткова відмінність полягає в тому, що кожне отримане повідомлення з зазначеної третьої підмножини спочатку виводять через відеоадаптер на дисплей тільки в графічному режимі, візуально ідентифікують як файл, що належить до першої зазначеної або до другої зазначеної підмножини, і далі:

а) потребу в кожному ідентифікованому текстовому і/або іконічному файлі оцінюють переглядом набору пікселів і

при позитивній оцінці - перетворюють набір пікселів в активному вікні дисплея в стандартний текстовий і/або графічний формат і це перетворене повідомлення безпосередньо з активного вікна дисплея записують у ДЗП комп'ютера, що захищається, і відповідний запис у ЗЗП стирають, а

при негативній оцінці - активне вікно дисплея закривають без зберігання даних і запис відповідного повідомлення у ЗЗП стирають; і/або

б) в імені кожного ідентифікованого програмного файла стандартне розширення заміняють нестандартним розширенням, виконують пробний запуск програми переважно поза комп'ютером, що захищається, оцінюють потребу в отриманій програмі і

при позитивній оцінці - записують прийняту програму в ДЗП комп'ютера, що захищається, і стирають запис висхідного повідомлення у ЗЗП, а

при негативній оцінці - стирають запис непотрібного висхідного повідомлення у ЗЗП.

Природно, що при такій обробці прийняті текстові і/або графічні файли будуть практич-

но звільнені від вірусів або програм злому, а прийняті програмні файли послужать «могильниками» для хробаків і/або троянських коней.

Поставлена задача вирішена також тим, що пристрій для захисту пам'яті комп'ютерів від несанкціонованого доступу, що має зовнішній відносно комп'ютера, що захищається, засіб для обміну даними між зовнішніми джерелами повідомлень і цим комп'ютером і щонайменше один зовнішній контролер для керування обробкою одержуваних повідомлень, який здатний розділяти дані, одержувані з зовнішніх джерел, і команди, що надходять від комп'ютера, що захищається, *згідно з винаходом:*

засіб для обміну даними між зовнішніми джерелами повідомлень і комп'ютером, що захищається, виконаний на основі щонайменше одного зовнішнього запам'ятовуючого пристрою (ЗЗП), який призначений для запису кожної чергової множини отриманих повідомлень і їх тимчасового збереження на термін обробки і який зв'язаний з зовнішніми джерелами повідомлень через керований вхідний перемикач,

зовнішній контролер керуючим виходом зв'язаний з зазначеним ЗЗП й оснащений власним програмним забезпеченням для обробки отриманих повідомлень, що записані на постійному запам'ятовуючому пристрої (ПЗП), а

на інформаційний вихід зазначеного ЗЗП підключений відеобуфер, що призначений для перетворення отриманих текстових і/або іконічних повідомлень у графічний формат і послідовного виведення перетворених повідомлень через керований вихідний перемикач на дисплей для тестування й прийняття рішення про прийом або відмову від прийому кожного повідомлення.

Такий пристрій відтинає ОЗП і ДЗП комп'ютера, що захищається, від зовнішніх джерел повідомлень на весь час прийому й обробки кожної чергової множини отриманих повідомлень. Далі, він слугує керованим буфером для посилки в зовнішні канали зв'язку тільки таких повідомлень із комп'ютера, що захищається, які схвалені законним користувачем, у такому режимі, коли ОЗП і ДЗП комп'ютера, що захищається, відключені від ЗЗП й у канал зв'язку відкритий тільки інформаційний вихід цього ЗЗП. Таким чином, навіть при прийомі програм, що заражені хробаками або троянськими конями, «діалог» комп'ютера, що захищається, зі сторонніми користувачами практично виключений.

Перша додаткова відмінність полягає в тому, що в режимі тестування отриманих повідомлень зазначений відеобуфер підключений до зазначеного дисплею через власний відеоадап-

тер комп'ютера, що захищається. Це скорочує апаратурні витрати на брандмауер.

Друга додаткова відмінність полягає в тому, що зазначене ПЗП включено між зазначеним контролером і зазначеним ЗЗП. Це дозволяє включити в брандмауер не тільки програми обробки отриманих повідомлень, але й емулятори операційних систем, необхідних для виконання істотної частини такої обробки усередині брандмауера.

Третя додаткова відмінність полягає в тому, що пристрій для захисту пам'яті комп'ютерів оснащено буфером команд, який через вхідний шлюз підключений на щонайменше один керуючий вихід комп'ютера, що захищається, і далі на керуючий вхід контролера і/або керуючий вхід ЗЗП. Це дозволяє за необхідністю компенсувати ушкодження або утрату власного ПО брандмауера в цілому або в частині або модифікувати таке ПО і, за бажанням користувача комп'ютера, що захищається, вручну управляти обробкою (тобто тестуванням і оцінкою) отриманих повідомлень.

Фахівцю зрозуміло, що при виборі конкретних варіантів здійснення винаходу можливі довільні комбінації зазначених додаткових відмінностей з основним винахідницьким задумом і що описані нижче кращі приклади його втілення ніяким чином не обмежують обсяг винаходу.

Короткий опис креслень

Далі суть винаходу пояснюється докладним описом пристрою і способу захисту від несанкціонованого доступу до пам'яті комп'ютерів з посиланнями на додане креслення, де зображена блок-схема пристрою для захисту пам'яті комп'ютерів від несанкціонованого доступу (далі ПЗПК).

Найкращі варіанти реалізації винахідницького задуму

ПЗПК має такі зовнішні стосовно комп'ютеру, що захищається, блоки:

керований вхідний перемикач 1 для підключення ПЗПК до довільного не позначеного особливо зовнішнього каналу зв'язку і відключення такого каналу на час обробки непустої множини отриманих повідомлень,

щонайменше один зовнішній запам'ятовуючий пристрій (ЗЗП) 2, інформаційний вхід якого зв'язаний з перемикачем 1 і який призначено для запису і тимчасового збереження кожної чергової множини отриманих повідомлень на час їх обробки,

зовнішній контролер 3, що оснащений власним програмним забезпеченням для обробки отриманих повідомлень і керуючим виходом зв'язаний з ЗЗП 2,

ПЗП 4, що включено між контролером 3 і ЗЗП 2 і слугує носієм згаданого власного ПО,

відеобуфер 5, що підключений на інформаційний вихід ЗЗП 2 і призначений для перетворення кожного з отриманих повідомлень у графічний формат і, за бажанням, для тимчасового збереження перетворених повідомлень до завершення тестування й ухвалення рішення про прийом або відмову від прийому кожного повідомлення,

керований вихідний перемикач 6 для підключення відеобуфера 5 на інформаційний вхід дисплея 7 комп'ютера 8, що захищається, з використанням, за бажанням, вбудованого в комп'ютер 8 відеоадаптеру 9.

Доцільно, щоб у складі ПЗПК був передбачений буфер 10 команд, що підключений через вхідний шлюз 11 на щонайменше один керуючий вихід (наприклад, клавіатури і/або миші) комп'ютера 8 і далі на керуючий вхід контролера 3 і/або керуючий вхід ЗЗП 2. Цей же буфер 10 може бути використаний для компенсації ушкоджень або втрат і для модифікації власного ПО ПЗПК у цілому або в окремих частинах і, за бажанням законного користувача комп'ютера 8, для ручного керування обробкою отриманих повідомлень.

Всі зазначені блоки можуть бути легко реалізовані фахівцями в галузі обчислювальної техніки на загальнодоступній елементній базі. Дійсно:

зовнішній контролер 3 може бути реалізований на базі довільних сучасних процесорів для персональних комп'ютерів, а

ЗЗП 2 і ПЗП 4 можуть бути виконані у вигляді звичних «блоків пам'яті тільки для читання (ROM)», енергонезалежних блоків пам'яті типу «EPROM», мікросхем пам'яті типу «FLASH», дисків типу «CD ROM» з відповідними лазерними дисководами, окремого дисковода з жорстким магнітним диском і їх довільної придатної комбінації.

Описаний пристрій працює як засіб виконання комплексу програм обміну даними між комп'ютером 8, що захищається, і довільним зовнішнім каналом зв'язку.

Так, програмне забезпечення для прийому й обробки повідомлень, що надходять із зовнішнього каналу зв'язку, як мінімум, включає наступні компоненти:

а) команду автоматичного запирання керованого вихідного перемикача 6 перед підключенням комп'ютера 8 до джерела повідомлень, наприклад, до *Internet*;

б) команду автоматичного запису усіх вхідних повідомлень у кожному сеансі зв'язку на щонайменше одне ЗЗП 2, замкнене з боку комп'ютера 8;

в) команду автоматичного запирання керованого вхідного перемикача 1 на інформаційному вході у ЗЗП 2 після припинення або переривання зв'язку з джерелом повідомлень;

г) програму переважно автоматичного сортування непустої множини отриманих повідомлень і виділення з неї щонайменше однієї непустої підмножини файлів, що належить до групи підмножин, яка складається з:

першої підмножини файлів, імена яких мають такі стандартні розширення, що вказують на текстовий і/або іконічний характер цих файлів, як «txt ; asc; rtf; doc; html; htm; bmp; jpg; gif; tif» і ін. і/або

другої підмножини файлів, імена яких мають такі стандартні розширення, що вказують на програмний характер цих файлів, як «exe; com; bat; log; sys; dat; dll; dot; chm; tlb; fon; pak; lsd; htf; ind; wdf; clf; swi» і ін. і/або

третьої підмножини файлів, імена яких мають нестандартні (звичайно присвоєні відправниками) розширення і які можуть бути віднесені до першої або другої з зазначених вище підмножин тільки після додаткового аналізу;

д) програми обробки повідомлень у кожній з зазначених підмножин для визначення потреби в їх одержанні і допустимості їх включення в БД і/або БЗ і/або ПО комп'ютера 8, що захищається.

Програма сортування завжди передбачає такі операції:

а) аналіз повних імен отриманих файлів;

б) порівняння фактичних розширень імен файлів з стандартними розширеннями;

в) виділення щонайменше однієї з зазначених вище підмножин (при тому, що в третю підмножину можуть бути включені файли, імена яких мають будь-які сумнівні розширення).

Програми обробки повідомлень специфічні для кожної з зазначених підмножин файлів і включають в основному автоматичні і, за необхідністю або за бажанням, ручні операції.

Так, програма обробки повідомлень у вигляді текстових і/або іконічних файлів з зазначеної першої підмножини, як мінімум, передбачає:

а) автоматичне перетворення кожного повідомлення в графічний формат, тобто в набір пікселів;

б) автоматичне виведення зазначеного набору пікселів через відеоадаптер на дисплей тільки в графічному режимі з застосуванням, за бажанням, стандартних команд керування екраном (при цьому цілком безпечно використання відеоадаптеру 9 і дисплея 7 в обхід ОЗП і ДЗП комп'ютера 8, що захищається);

в) оцінку потреби в отриманому повідомленні, яку звичайно робить законний користувач

комп'ютера 8, що захищається шляхом візуального перегляду тексту і/або зображення в активному вікні дисплея;

г) подачу (звичайно вручну) команди або на прийняття, або на відмову від прийняття повідомлення;

д) звичайно автоматичне перетворення набору пікселів, що відповідає прийнятому повідомленню, у придатний стандартний текстовий і/або графічний формат і

е) автоматичний або ручний запис прийнятого повідомлення в текстовому і/або іконічному форматі безпосередньо з активного вікна дисплея під прийнятним ім'ям у ДЗП комп'ютера 8, що захищається, і автоматичне ініціювання команди на стирання відповідного запису у ЗЗП 2, *або*

ж) переважно автоматичне закриття активного вікна дисплея, що містить набір пікселів, який відповідає відкиненому повідомленню, без зберігання даних і автоматичне ініціювання команди на стирання відповідного запису у ЗЗП 2;

з) автоматичне стирання прийнятого або відкиненого повідомлення у ЗЗП 2 після операції (е) або операції (ж), яке виконується, залежно від установки, негайно або з довільною затримкою (аж до завершення обробки всіх повідомлень, записаних у ЗЗП 2 в одному сеансі зв'язку).

Програма обробки повідомлень у вигляді програмних файлів з зазначеної другої підмножини, як мінімум, передбачає:

а) звичайно автоматичну заміну стандартного розширення імені кожного отриманого програмного файла нестандартним розширенням;

б) переважно ручний пробний запуск програмного файла зі зміненим ім'ям переважно поза комп'ютером 8, що захищається (зокрема, усередині ПЗПК за допомогою контролера 3 і ПЗП 4);

в) оцінку потреби в отриманому повідомленні, яку звичайно робить законний користувач комп'ютера 8 шляхом дослідження результатів зазначеного пробного запуску;

г) подачу (звичайно вручну) команди або на прийняття, або на відмову від прийняття програмного повідомлення;

д) переважно ручний запис прийнятої програми (переважно з новим ім'ям) у ДЗП комп'ютера 8 й автоматичне ініціювання команди на стирання відповідного запису у ЗЗП 2, *або*

е) автоматичне ініціювання команди на стирання запису відкиненого програмного повід-

омлення у ЗЗП 2 і

ж) автоматичне стирання прийнятого або відкиненого повідомлення у ЗЗП 2 після операції (д) або операції (е), яке виконується, залежно від установки, негайно або з довільною затримкою (аж до завершення обробки всіх повідомлень, записаних у ЗЗП 2 в одному сеансі зв'язку).

Програма обробки повідомлень, що представляють собою невизначені файли з зазначеної третьої підмножини, як мінімум, передбачає:

а) автоматичне перетворення кожного невизначеного повідомлення в графічний формат, тобто в набір пікселів;

б) автоматичне виведення зазначеного набору пікселів через відеоадаптер на дисплей тільки в графічному режимі з застосуванням, за бажанням, стандартних команд керування екраном (при цьому цілком безпечно використання відеоадаптеру 9 і дисплеєм 7 в обхід ОЗП і ДЗП комп'ютера 8, що захищається);

в) ідентифікацію кожного чергового повідомлення або як файла, що належить до першої зазначеної підмножини, або як файла, що належить до другої зазначеної підмножини, і далі:

або виконання операцій (в)-(з) описаної вище програми обробки текстових і/або іконічних файлів для кожного виявленого файла такого типу,

або виконання всіх операцій описаної вище програми обробки кожного виявленого програмного файла.

Істотною частиною брандмауера відповідно до винаходу є програма виведення повідомлень із комп'ютера 8, що захищається, у зовнішній канал зв'язку. Вона включає:

а) подавану вручну команду на підключення комп'ютера 8, що захищається, до зовнішнього каналу зв'язку, що приводить до запирання обох перемикачів 1 і 6;

б) реалізовані через вхідний шлюз 11 і буфер 10 команди автоматичної перевірки відсутності записів у ЗЗП 2 після попереднього сеансу зв'язку й автоматичного очищення ЗЗП 2, якщо за якимись причинами непотрібні записи залишилися;

в) звичайно вручну виконувану команду на запис призначених до відправлення повідомлень, які надходять у ЗЗП 2 через вхідний шлюз 11 і буфер 10;

г) команду автоматичного відмикання перемикача 1, виконувану після завершення запису у ЗЗП 2;

д) команду на відправлення повідомлень у зовнішній канал зв'язку, що звичайно автома-

тично виконується при замкнених перемикачі 6 і шлюзі 11.

Промислова придатність

Винахід промислово придатний, тому що:

пристрій для захисту пам'яті комп'ютерів від несанкціонованого доступу може бути легко реалізований на загальнодоступній елементній базі,

здійснюваний за допомогою пристрою спосіб забезпечує практично непробивний захист від злому БД і/або БЗ і/або ПО комп'ютерів, що захищаються.

За дорученням В.Л. Куцевич

ФОРМУЛА ВИНАХОДУ

1. Спосіб захисту пам'яті комп'ютерів від несанкціонованого доступу, що заснований на поділі даних, одержуваних по загальнодоступних каналах зв'язку, і команд керування обробкою даних, що надходять від комп'ютера, що захищається, з застосуванням зовнішніх апаратних засобів, який відрізняється тим, що

а) у кожному сеансі зв'язку усі вхідні повідомлення спочатку записують на щонайменше один замкнений з боку комп'ютера, що захищається, зовнішній запам'ятовуючий пристрій (далі ЗЗП);

б) потім замикають вхід у ЗЗП з боку каналу зв'язку;

в) під керуванням зовнішнього контролера з власним програмним забезпеченням незалежно від ЦП, ДЗП й ОЗП комп'ютера, що захищається, сортують непусту множину отриманих повідомлень і виділяють із неї щонайменше одну непусту підмножину файлів, яка належить до групи підмножин, що складається з:

першої підмножини файлів, імена яких мають стандартні розширення, що вказують на текстовий і/або іконічний характер цих файлів, і/або

другої підмножини файлів, імена яких мають стандартні розширення, що вказують на програмний характер цих файлів, і/або

третьої підмножини файлів, імена яких мають нестандартні розширення і які можуть бути віднесені до першої або другої з зазначених підмножин після додаткового аналізу; і

г) під керуванням зазначеного зовнішнього контролера також незалежно від ЦП, ДЗП й ОЗП комп'ютера, що захищається, обробляють повідомлення в кожній з зазначених підмножин для визначення потреби в їх одержанні і допустимості їх включення у БД і/або БЗ і/або ПО комп'ютера, що захищається.

2. Спосіб за п.1, який відрізняється тим, що кожне отримане повідомлення, що є текстовим і/або іконічним файлом із зазначеної першої підмножини, виводять через відеоадаптер на дисплей тільки в графічному режимі у вигляді набору пікселів, оцінюють потребу в отриманому повідомленні і далі:

при позитивній оцінці - перетворюють набір пікселів в активному вікні дисплея в стандартний текстовий і/або графічний формат і це перетворене повідомлення безпосередньо з активного вікна дисплея записують у ДЗП комп'ютера, що захищається, і відповідний запис у ЗЗП стирають, а

при негативній оцінці - активне вікно дисплея закривають без зберігання даних і запис відповідного повідомлення у ЗЗП стирають.

3. Спосіб за п.2, який **відрізняється** тим, що зазначений набір пікселів, що представляє текстовий і/або іконічний файл, формують з використанням стандартних команд керування екраном.

4. Спосіб за п.2 або п.3, який **відрізняється** тим, що використовують відеоадаптер і дисплей комп'ютера, що захищається.

5. Спосіб за п.1, який **відрізняється** тим, що в імені кожного програмного файла з зазначеної другої підмножини стандартне розширення заміняють нестандартним розширенням, виконують пробний запуск такого файла переважно поза комп'ютером, що захищається, оцінюють потребу в отриманій програмі і далі:

при позитивній оцінці - записують прийняту програму в ДЗП комп'ютера, що захищається, і стирають запис висхідного повідомлення у ЗЗП, а

при негативній оцінці - стирають запис непотрібного висхідного повідомлення у ЗЗП.

6. Спосіб за п.1, який **відрізняється** тим, що кожне отримане повідомлення з зазначеної третьої підмножини спочатку виводять через відеоадаптер на дисплей тільки в графічному режимі, візуально ідентифікують як файл, що належить до першої зазначеної або до другої зазначеної підмножини, і далі:

а) потребу в кожному ідентифікованому текстовому і/або іконічному файлі оцінюють переглядом набору пікселів і

при позитивній оцінці - перетворюють набір пікселів в активному вікні дисплея в стандартний текстовий і/або графічний формат і це перетворене повідомлення безпосередньо з активного вікна дисплея записують у ДЗП комп'ютера, що захищається, і відповідний запис у ЗЗП стирають, а

при негативній оцінці - активне вікно дисплея закривають без зберігання даних і запис відповідного повідомлення у ЗЗП стирають; і/або

б) в імені кожного ідентифікованого програмного файла стандартне розширення заміняють нестандартним розширенням, виконують пробний запуск програми переважно поза комп'ютером, що захищається, оцінюють потребу в отриманій програмі і

при позитивній оцінці - записують прийняту програму в ДЗП комп'ютера, що захищається, і стирають запис висхідного повідомлення у ЗЗП, а

при негативній оцінці - стирають запис непотрібного висхідного повідомлення у ЗЗП.

7. Пристрій для захисту пам'яті комп'ютерів від несанкціонованого доступу, що має зовнішній відносно комп'ютера, що захищається, засіб для обміну даними між зовнішніми джерелами повідомлень і цим комп'ютером і щонайменше один зовнішній контролер для керування обробкою одержуваних повідомлень, який здатний розділяти дані, одержувані з зовнішніх джерел, і команди, що надходять від комп'ютера, що захищається, який відрізняється тим, що

засіб для обміну даними між зовнішніми джерелами повідомлень і комп'ютером, що захищається, виконаний на основі щонайменше одного зовнішнього запам'ятовуючого пристрою (ЗЗП), який призначений для запису кожної чергової множини отриманих повідомлень і їх тимчасового збереження на термін обробки і який зв'язаний з зовнішніми джерелами повідомлень через керований вхідний перемикач,

зовнішній контролер керуючим виходом зв'язаний з зазначеним ЗЗП й оснащений власним програмним забезпеченням для обробки отриманих повідомлень, що записані на постійному запам'ятовуючому пристрої (ПЗП), а

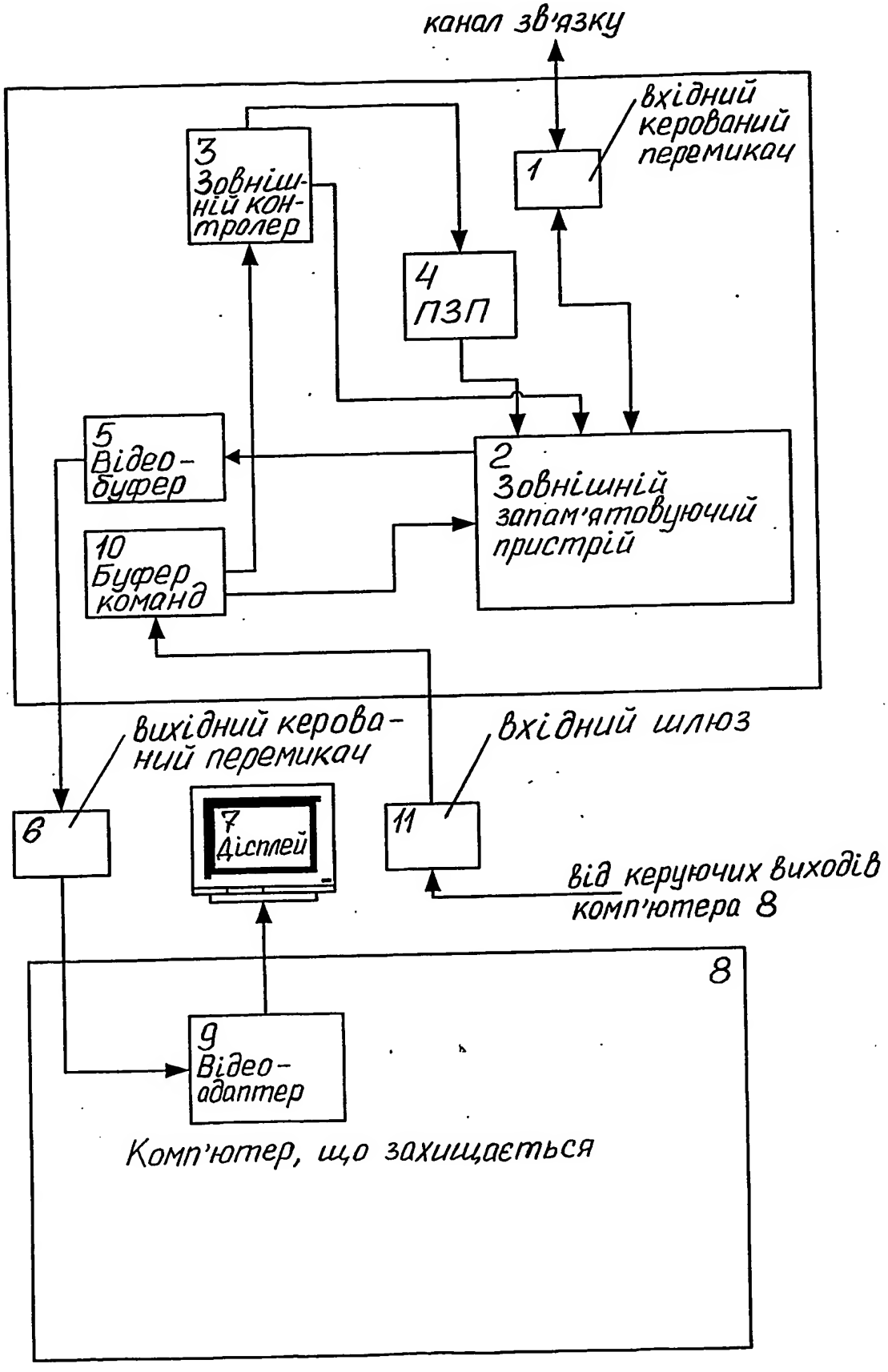
на інформаційний вихід зазначеного ЗЗП підключений відеобуфер, що призначений для перетворення отриманих текстових і/або іконічних повідомлень у графічний формат і послідовного виведення перетворених повідомлень через керований вихідний перемикач на дисплей для тестування й прийняття рішення про прийом або відмову від прийому кожного повідомлення.

8. Пристрій за п.7, який відрізняється тим, що в режимі тестування отриманих повідомлень зазначений відеобуфер підключений до зазначеного дисплею через власний відеоадаптер комп'ютера, що захищається.

9. Пристрій за п.7, який відрізняється тим, що зазначене ПЗП включено між зазначеним контролером і зазначеним ЗЗП.

10. Пристрій за п.7, який відрізняється тим, що він оснащений буфером команд, який через вхідний шлюз підключений на щонайменше один керуючий вихід комп'ютера, що захищається, і далі на керуючий вхід контролера і/або керуючий вхід ЗЗП.

За дорученням В.Л. Куцевич


канал зв'язку
вхідний керований перемикач
1
3 Зовнішній контролер
4 ПЗП
5 Відео-буфер
2 Зовнішній запам'ятовуючий пристрій
10 Буфер команд
вихідний керований перемикач
вхідний шлюз
6
7 Дісплей
11
від керуючих виходів комп'ютера 8
8
9 Відео-адаптер
Комп'ютер, що захищається

РЕФЕРАТ

СПОСІБ ЗАХИСТУ ПАМ'ЯТІ КОМП'ЮТЕРІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ передбачає поділ даних, одержуваних по каналах зв'язку, і команд керування обробкою даних, що надходять від комп'ютера, що захищається, за допомогою зовнішнього контролера. Для практичного виключення пробою брандмауера всі отримані в сеансі зв'язку повідомлення записують на ЗЗП, яке замкнене з боку комп'ютера, що захищається, замикають вхід у ЗЗП і незалежно від ЦП, ДЗП й ОЗП комп'ютера, що захищається, сортують повідомлення на текстові і/або іконічні файли, програмні файли і файли невизначеного типу і роздільно визначають потребу в отриманих файлах і допустимість їх використання в комп'ютері, що захищається.

ПРИСТРІЙ ДЛЯ ЗДІЙСНЕННЯ СПОСОБУ має підключене до зовнішнього контролера ЗЗП і вхідний і вихідний керовані перемикачі.

2 н.з.п.ф; 8 з.п.ф.; 1 іл.